OVERSIGHT

EH2PUB/03-98/02SR

Interim Status Report on Limited Review of

Department of Energy Unclassified Computer Systems

March 1998

DEPARTMENT OF ENERGY
UNITED STATES OF AMERICA

Office of Oversight

Environment
Safety
Health
Safeguards
Security

Office of Environment, Safety and Health

TABLE OF CONTENTS

Abbreviations Used in This Report

CRADA	Cooperative Research and Development Agreement
DOE	U.S. Department of Energy
FTP	File Transfer Protocol
OUO	Official Use Only
UCNI	Unclassified Controlled Nuclear Information

OVERSIGHT

1.0 Introduction

As part of the ongoing effort of the Department of Energy (DOE) Office of Oversight, the Office of Security Evaluations is conducting a review of selected unclassified computer systems at all major DOE facilities. The primary purpose of the review is to evaluate DOE's protection of national security-related information. The review involves remotely scanning various systems from a location outside each DOE site. This process allows Oversight to determine whether site programs are adequate to ensure that national security-related information, such as Unclassified Controlled Nuclear Information (UCNI) and Official Use Only (OUO) information, is not contained on systems that are freely accessible over the Internet. It also enables Oversight to determine whether intruders can use vulnerabilities in Internet-accessible systems to access systems containing classified or national security-related unclassified information. While the review is primarily intended to identify vulnerabilities and provide line managers with the information they need to improve the security and integrity of information related to national security, the Oversight scans also identify vulnerabilities involving other sensitive information that should not be accessible to the general public, such as salary data, individual radiation exposure records, and Cooperative Research and Development Agreement (CRADA) documents. Such weaknesses are also communicated to line managers so that appropriate action can be taken.

Scanning focuses on DOE systems connected to the Internet that allow open, "anonymous" access.

The Security Evaluations scanning focuses exclusively on DOE systems connected to the Internet that allow open, "anonymous" access. Because these particular systems permit anyone with access to the Internet to view information from virtually anywhere in the world, it is important that only information intended to be shared with the world is placed on these systems, and that appropriate and effective restrictions be applied to the system files that are not intended for worldwide distribution.

The review is approximately 50 percent complete. However, Security Evaluations believes it is appropriate to share with the DOE complex the general results of the review to date, especially given the seriousness of some of the problems observed thus far.

2.0 Methodology

For this review, Security Evaluations uses an automated scanning tool that identifies computer systems configured as file transfer protocol (FTP) servers. Once such servers are identified, the scanning tool then automatically attempts to log on to each system by employing the user name "anonymous." If a system allows logon via this "anonymous access," the user is granted access to that system, whereupon he/she then enters any electronic mail (e-mail) address (not necessarily a real address) when prompted for a password. Once the scanning tool identifies the systems that can be accessed anonymously, Security Evaluations manually explores those systems to determine the extent to which an anonymous user could readily read, upload, delete, or otherwise modify any of the information accessed.

Security Evaluations is cautious not to erase data, damage any system, or compromise any data while conducting the scans.

The scanning is conducted under a number of self-imposed restrictions. Under these restrictions, Security Evaluations is cautious not to erase data, damage any system in any way, or compromise the confidentiality of any data (beyond what the system already allows) while conducting the scans. Security Evaluations does not engage in many of the activities commonly associated with hacking, such as deleting/altering data or uploading a "sniffer" specifically designed to steal passwords. In fact, Security Evaluations scanning only simulates what a relatively unsophisticated user could readily accomplish, such as using exposed passwords to access a system by posing as an authorized user; therefore, the scanning by no means represents either a severe test of the system or the full extent of malicious activities that can occur. It must also be recognized that the scope of review activities for each facility is limited to only a very small "slice in time." That is, the results of scanning merely identify the systems and data that could be accessed in a finite time frame, and may not represent what data, or types of data, might have been accessible to anonymous users in the past, or could be available in the future. Despite Security Evaluations' self-imposed restrictions, the scanning is very realistic and useful in providing a perspective on the effectiveness of system controls and on informing site management as to what kind of information resides on its systems and is freely available to Internet users worldwide.

3.0 Results

Many of DOE's anonymous FTP servers are not securely configured.

The scanning showed that many of DOE's anonymous FTP servers are not securely configured. Problems range generally from susceptibility of the servers as hacker drop-off points for illegally obtained software, to allowing anonymous user access to critical system configuration files (which, once accessed, permit further access to more powerful system files/ accounts). Although each site has unique characteristics and problems, the key result of this effort is that sites need to have both effective barriers (e.g., firewalls) and effective procedures to control the establishment of anonymous FTP servers.

The results of this review demonstrate that:

- At sites where anonymous FTP servers are limited in number and/or controlled by system administrators, appropriate barriers, and prescribed procedures, few problems are experienced. Thus, at sites where barriers such as firewalls are effectively employed and where system users must obtain permission from administrators to establish anonymous FTP servers, few problems or vulnerabilities arise.

- Conversely, at sites having a significant number of anonymous FTP servers and no associated barriers or administrative controls (i.e., no firewalls and procedures to limit or control anonymous FTP servers), many exploitable system vulnerabilities are evident.

The following paragraphs discuss the various specific problems observed to date. These are grouped into three vulnerability categories: (1) those that allow anonymous Internet users to access files with content that is inappropriate for the public domain; (2) those associated with the ability to read, write, and alter file contents; and (3) those that resulted in compromise of user accounts.

Inappropriate File Contents

DOE policy clearly requires that the level of protection be appropriate for the type of information. For example, there are very stringent requirements for processing Top Secret matter and other classified information. Such information must, of course, never be placed on unclassified systems. Likewise, sensitive unclassified data–for example, UCNI or OUO information–also requires substantial protection, but less than that for classified data. Other sensitive unclassified information requires an appropriate degree of protection as well.

Ideally, computer systems at DOE sites should process only the type of information for which they have been approved. That is, a computer system approved for processing budget data should not be used for UCNI or classified information. Similarly, a system that is open to anonymous users anywhere in the world should contain only information suitable for general release and should not contain sensitive or classified data. Inherent in this concept is the need for effective processes to ensure that systems contain only information commensurate with the degree of protection provided. However, the Security Evaluations scans demonstrate that such DOE processes are not uniformly effective. In practice, these processes do not ensure that information placed on DOE computer systems has been adequately reviewed and determined to be appropriate for those systems before being put there.

One of the most significant problems noted during the review is that some sites do not have effective processes for ensuring that classified and sensitive information is not contained on computer systems that are accessible over the Internet. In many cases, the computer system users have no controls and little training as to what can and cannot be placed on a particular system. At one site, Security Evaluations identified several files that appeared to contain highly sensitive information. These files were initially reviewed by a trained and qualified classification official and determined to contain classified information. In accordance with DOE procedures, the Office of Declassification, within the Office of Nonproliferation and National Security, was informed of the situation and asked to perform an additional review to determine the classification of the potentially classified documents, and the site was informed so that appropriate action could be taken. After several weeks and various conflicting opinions, the Office of Declassification has completed the review of the documents and determined that one document is indeed classified. The sites involved have since modified their systems so that such documents are no longer accessible by anonymous users. However, the fact that such information was accessible to anyone with an Internet connection remains a significant concern. This situation highlights the need for effective procedures and for well trained computer users who are aware of their security responsibilities.

Unclassified Controlled Nuclear Information and Official Use Only information was found on anonymous servers.

In addition, the following types of sensitive unclassified information were found to be available to anonymous users.

Unclassified Controlled Nuclear Information. Accessing one system as an anonymous Internet user, Security Evaluations personnel copied several UCNI-marked documents, including:

- Documents providing detailed descriptions (hundreds of pages) of a facility containing special nuclear material, including building configurations, process descriptions, and routes by which materials are moved
- Lists of employees who have authorized access into restricted areas
- A document containing the step-by-step procedures for working in a process glovebox

- An UCNI drawing that was part of a larger document, which provided details about a research project.

Export-Controlled Information. A Department of Defense software package (computer code) was downloaded in its entirety. The distribution agreement for this package states that "This material contains technical data the export of which is restricted by statute. Violations may result in administrative, civil, or criminal penalties. Distribution of this material is limited to the Department of Energy, the Department of Defense, and approved contractors thereof."

Cooperative Research and Development Agreement Information. These documents included project planning files and reports involving CRADA-related project information.

Official Use Only Information. Files containing detailed project schedules, workshop reports, and other documents marked as OUO were downloaded.

DOE-defined Sensitive Documents. Although not specifically marked as being sensitive, documents were downloaded that fall into one or more categories of sensitive information, as defined in the DOE guidelines:

- Personal dosimetry reports.
- Subcontract Performance Appraisals, including information on fees and penalties.
- Salary spreadsheets for employees (marked "In Confidence").
- Employee performance appraisals and salary justification memos.
- System Password Files. In several cases, user passwords were cracked, granting full access to user files and programs. Also, many e-mail passwords were revealed, some of which allowed interactive access to large e-mail servers where user data directories were available for downloading. Using the same compromised e-mail passwords, Security Evaluations personnel copied several other password files and subjected them to a cracking program. By cracking passwords and subsequently using the compromised accounts to copy other systems' password files, an intruder could migrate throughout a network and obtain additional sensitive information.

In each of the instances above, the sites were notified that UCNI, OUO, or other sensitive documents were accessible by an anonymous user. In each case, the sites took action to ensure that specific documents were no longer accessible, usually by removing the document file from the system or by discontinuing anonymous access authorization.

Read, Write, and Alter Vulnerabilities

Many DOE systems are susceptible to being used by hacker groups to distribute illegal software.

Many file transfer servers are configured to allow anonymous users to write to the system disk and subsequently read back the data. In doing so, users can not only access and view a given file, but can also introduce new text or graphics into that file and/or alter the file's existing content.

Susceptibility to Illicit Use. Some systems are susceptible to being used by hacker groups to distribute software, passwords (to other compromised systems), and lists of other systems currently used to distribute illegal software. In fact, Security Evaluations noted one case where pirated software was present on a DOE system. Once a server is used for this purpose, it is often referenced in a "pirate list" of compromised sites. These lists are distributed throughout the Internet "underground" and are used by hackers to locate sites containing the illegally obtained software or hacking tools they seek. In addition to the potential for embarrassing DOE, this can lead to untimely interruption of service due to excessive use by hackers.

Windows NT Default Configuration. Anonymous access is allowed when default configuration parameters are used. While this default anonymous access is limited to reading documents from a specific FTP directory on a hard drive, files not intended for the public may be placed into the directory unintentionally. In one instance, Security Evaluations personnel copied a user's entire e-mail inbox that was available on the FTP directory.

Macintosh Versaterm Default Configuration. The default configuration for Versaterm FTP servers enables anonymous "read" access to the main system directory. Although anonymous users cannot change directories, they can read any file contained in the main directory. In many cases, the main directory contains the virtual memory file (called VM Storage), which contains current and recent data that the system has processed. Some VM Storage files that Security Evaluations personnel were able to access contained sensitive working documents, e-mail, passwords, and other potentially sensitive information that could be downloaded by an anonymous user.

Some DOE World Wide Web servers can be modified from the Internet by anonymous users.

Web Pages Subject to Tampering. Some systems that provide access to various site Web pages allow anonymous users to alter the content of existing pages, or to add additional information or pictures to the pages. This could lead to an embarrassing incident if hackers were to modify any of the pages to present pornographic or anti-government information. Incidents such as these are becoming more common, as illustrated by the recent problems experienced by the Department of Justice, the Air Force, and the Central Intelligence Agency. Additionally, anonymous users can write to the directory where executable programs are stored and can upload malicious programs, which could then be unknowingly executed by legitimate system users.

User Account Compromise

Using information obtained through anonymous access, hackers could migrate throughout the network, eventually accessing more sensitive information.

Using information obtained through anonymous access, Security Evaluations personnel were able to compromise user accounts on several systems. It should be noted that the self-imposed restrictions prevented Security Evaluations personnel from attempting to gain access to additional sensitive information by exploiting potential operating system vulnerabilities associated with these systems. However, a hacker could readily achieve a higher level of access, install a keystroke logger (sniffer), and easily capture account information and passwords for other computers at a given site. The hacker could then migrate throughout the network, eventually accessing more sensitive information. The passwords for these accounts were obtained through three means:

1. Password files that were accessible by anonymous users (although some accounts did not even require passwords to log on). Security Evaluations personnel copied the password files and subjected them to a "cracking" program, which decrypted several passwords. Some of the passwords were verified to grant access to other areas of the systems from which they were obtained, as well as interactive (telnet) access to other systems. In fact, some of these other systems do not allow anonymous access at all. However, because the system treats these passwords as coming from onsite users rather than from anonymous users, Security Evaluations was able to access information not intended to be released to the world.

2. Software configuration files that were available to anonymous users. For example, a popular FTP software package (WS_FTP) stores passwords for other systems in its configuration file. By copying the configuration file to the Security Evaluations scanning system, Security Evaluations personnel were able to access systems that do not allow anonymous access. Once inside the systems, Security Evaluations personnel copied the password files, which, when subjected to the cracking program, yielded valid passwords.

3. System configuration files in user directories. One of the files (.RHOSTS) shows other systems for which each user has an account.

Security Evaluations personnel then used the users' passwords to access these other systems. Because many users employ the same password for multiple systems, this provided access to systems not intended to be placed in the public domain.

4.0 Conclusions and Opportunities for Improvement

Effective use of firewalls can prevent many of the problems found during this study.

The results to date clearly show that virtually anyone on the Internet could use a simple scanning tool to gain access to, at a minimum, password files and, more disconcerting, classified and sensitive data. Results also revealed that hackers can and have compromised DOE systems and that systems are vulnerable to serious malicious activity, including introduction of viruses and Trojan horse software, deletion of government data, or further penetration of DOE networks.

Lists of the vulnerable anonymous FTP servers have been provided to each site visited thus far so that computer security administrators can identify which servers were found to be vulnerable and why, and can implement corrective measures accordingly. To date, these combined lists show that numerous DOE servers were found to have one or more of the aforementioned vulnerabilities. How, when, how often, or by whom these vulnerabilities and data may have already been exploited via the worldwide Internet can only be conjectured. Moreover, given that Internet users, and hackers in particular, are not subject to the self-imposed restrictions of this review, it is unknown what malicious activities may have already occurred in terms of the observed vulnerabilities.

As mentioned previously, at sites where barriers such as firewalls are effectively employed and where system users must obtain permission from administrators to establish anonymous FTP servers, fewer problems and vulnerabilities arise. Effective use of firewalls can prevent many of the problems described above, placing anonymous FTP servers under the direct control of system security administrators. Thus, the firewall should be considered a starting point for enhancing security.

Configuring a system for anonymous access, if done properly, does not necessarily create a problem in itself. However, when setting up an anonymous-access Internet server, two assurances should be made. First, only information that can be shared with the world should be placed on the server. Second, all directories that are accessible should be restricted to "read-only" access. If "write" access is necessary, it should be provided in a secure manner. The following should be considered when configuring a secure anonymous file transfer server:

- Any information to be made available to anonymous users should be thoroughly reviewed, and file restrictions should be configured accordingly.

- The password file used in the "ftp/etc" area should not contain valid passwords for the system.

- Anonymous users should not have the ability to delete or alter files.

- Incoming files should be placed into a protected "holding area" until the information can be evaluated and put into the public directories by system administrators. The DOE main file transfer server, FTP.DOE.GOV, is a good example of a properly configured server.

- The amount of data transferred in one session should be limited.

- System logging should be increased to allow early detection of abuse.

More detailed information regarding proper file server configuration can be found through various sources on the Internet, including the DOE Computer Incident Advisory Capability (CIAC).